PATENT APPLICATION

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re application of	Docket No: Q80686
Emmanuel MARILLY, et al.	
Appln. No.: 10/809,521	Group Art Unit: 2157
Confirmation No.: 7535	Examiner: Blake J. RUBIN
Filed: March 26, 2004	

For: A LOCAL ASSURANCE MANAGEMENT DEVICE FOR AN EQUIPMENT ELEMENT IN A COMMUNICATION NETWORK

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellant submits the following:

Table of Contents

I. REAL PARTY IN INTEREST

The real party in interest is ALCATEL of Paris France, the assignee. The assignment was recorded by the Assignment branch of the U.S. Patent and Trademark Office on March 26, 2004 (at Reel 015154, Frame 0009). It is noted that the name of the assignee is now ALCATEL-LUCENT.

II. RELATED APPEALS AND INTERFERENCES

A Notice of Appeal and Pre-Appeal Brief Request for Review was filed on September 22, 2008, in response to the Advisory Action dated September 10, 2008. In response to the filing of the Notice of Appeal and Pre-Appeal Brief Request for Review, the Notice of Panel Decision from Pre-Appeal Brief Review was mailed on December 9, 2008. The Notice of Panel Decision from Pre-Appeal Brief Review indicated that the application remains under appeal because there is at least one actual issue for Appeal.

To the knowledge and belief of Appellants, the Assignee, and the undersigned, there are no other appeals or interferences before the Board of Appeals and Interferences that will directly affect or be affected by the Board's decision in the instant Appeal.

III. STATUS OF CLAIMS

This Application was originally filed with claims 1-33 which are the subject of this appeal. Further, claims 1-33 stand finally rejected.

Claims 1-33 stand rejected under 35 U.S.C. 102(e) as being allegedly anticipated by Sistanizadeh et al. (U.S. 6,681,232; hereinafter "Sistanizadeh").

The rejections of claims 1-33 are being appealed.

No other grounds of rejection are currently pending.

A copy of the pending claims on appeal is set forth in the attached Appendix.

IV. STATUS OF AMENDMENTS

As of the Advisory Action dated September 10, 2008, the Examiner has entered the claim amendments of the Amendment under 37 C.F.R. 1.116 filed August 22, 2008, and no outstanding amendments to the claims are currently pending. Thus the claims stand as presented prior to the Advisory Action dated September 10, 2008. Therefore, all amendments and arguments are believed to have been previously entered and made of record.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The instant application is directed to a device and method enabling local assurance management operated by the network management system of a communication network.

Independent claim 1 is directed to a local assurance management device[1] for a network element[2] in a communication network[3] equipped with a network management system[4], where said network element presents a chosen configuration[5] and comprises means for measuring parameter values[6] in the network[7], and a built-in management information base[8] used to store management data which are representative of said measured parameter values[9], wherein the device comprises

management means[10] which are arranged to adapt the configuration of said network element[11] according to at least said management data stored in said management information

[1] See FIG. 2, element D; and page 8, line 2.

[2] See FIG. 2, element NE; and page 8, lines 3-7.

[3] See FIG. 1, element N; and page 6, lines 4-10.

[4] See FIG. 1, element NMS; and page 6, lines 10-11.

[5] See page 8, lines 10-11.

[6] See page 7, lines 11-30; and FIG. 2, element MM.

[7] See page 7, lines 20-23.

[8] See FIG. 2, element MIB.

[9] See page 8, lines 24-25.

[10] See page 8, lines 7-11; and FIG. 2, element MAE.

base[12], and chosen rules, known as assurance rules, defining a local assurance policy[13], where said adaptation comprises a change to a measurement policy parameter and/or a change to a report transmission policy to said network management system[14].

Claim 2 is directed to a device according to claim 1, wherein said management means[15] are arranged so as to adapt said configuration according to information data coming from at least one other network element[16].

Claim 3 is directed to a device according to claim 1, wherein said adaptation comprises a change to a method of operation of said network element[17].

Claim 4 is directed to a device according to claim 1, wherein said management means[18] include analysis means[19] arranged so as to determine, in accordance with certain of said chosen assurance rules, information data representing the changes in time, over a chosen interval, of parameter values in the network stored in said management information base[20].

[11] See page 8, lines 7-11; and FIG. 2, element MAE.

[12] See page 8, lines 15-21; and FIG. 2, element MIB.

[13] See page 8, lines 22-25.

[14] See page 8, lines 15-22; and FIG. 2, element NMS.

[15] See page 8, lines 7-11; and FIG. 2, element MAE.

[16] See page 8, lines 25-27.

[17] See page 8, lines 15-22; FIG. 2, element NE.

[18] See page 8, lines 7-11; and FIG. 2, element MAE.

[19] See page 9, line 8; and FIG. 2, element SM1.

[20] See page 9, lines 8-15; and FIG. 2, element MIB.

Claim 5 is directed to a device according to claim 4, wherein said analysis means[21] are arranged so as to deliver information data representing a trend analysis[22] and/or an analysis of profiles or signatures[23] and/or an analysis of discontinuity[24] and/or an aggregation of network parameter values[25].

Claim 6 is directed to a device according to claim 4, wherein said analysis means[26] are configurable[27].

Claim 7 is directed to a device according to claim 6, wherein said analysis means[28] are arranged so as perform fresh calculations relating to the network parameters[29] received from said network management system[30].

Claim 8 is directed to a device according to claim 1, wherein said management means[31] include alarm means[32] able to trigger the sending of an alarm and/or of information data[33] to said

[21] See page 9, line 8; and FIG. 2, element SM1.

[22] See page 9, lines 8-9.

[23] See page 9, lines 16-17.

[24] See page 9, lines 21-22.

[25] See page 9, lines 27-29.

[26] See page 9, line 8; and FIG. 2, element SM1.

[27] See page 10, line 35 - page 11, line 3.

[28] See page 9, line 8; and FIG. 2, element SM1.

[29] See page 13, lines 10-12.

[30] See FIG. 2, element NMS.

[31] See page 8, lines 7-11; and FIG. 2, element MAE.

network management system[34] and/or to at least one other network element, in accordance with certain of said chosen assurance rules[35].

Claim 9 is directed to a device according to claim 8, wherein said alarm means[36] are configurable.

Claim 10 is directed to a device according to claim 8, wherein said information data and said alarms are representative of the results of analyses performed by an analysis means[37], and/or of data aggregation, effected by said analysis means[38], and/or of a network parameter value stored in said management information base[39].

Claim 11 is directed to a device according to claim 1, wherein said management means[40] include network observation means[41] defining a flow measurement agent of the end-to-end

[32] See FIG. 2, element SM2.

[33] See page 10, lines 17-22; and FIG. 2, element SM2.

[34] See page 10, line 26; and FIG. 2, element NMS.

[35] See page 11, lines 26-28; and FIG. 2, element NE.

[36] See page 10, lines 17-22; and FIG. 2, element SM2.

[37] See page 9, line 8; and FIG. 2, element SM1.

[38] See FIG. 2, element SM1.

[39] See FIG. 2, element MIB.

[40] See page 8, lines 7-11; and FIG. 2, element MAE.

[41] See FIG. 2, element SM3.

type[42], arranged so as to determine information data which are representative of said flow of the end-to-end type in accordance with certain of said chosen assurance rules[43].

Claim 12 is directed to a device according to claim 11, wherein said network observation means are configurable[44].

Claim 13 is directed to a device according to claim 1, wherein said management means[45] include means for the management of service level agreements or SLAs[46], arranged so as to determine information data representing said agreement management in accordance with certain of said chosen assurance rules[47].

Claim 14 is directed to a device according to claim 13, wherein said service level agreement management means[48] are configurable.

Claim 15 is directed to a device according to claim 2, wherein said management means[49] include monitoring means[50] which are able to manage the operation of an analysis means[51], of an

[42] See page 11, lines 8-10; and FIG. 2, element SM3.

[43] See page 11, lines 11-16.

[44] See page 11, lines 1-3; and FIG. 2, element SM3.

[45] See page 8, lines 7-11; and FIG. 2, element MAE.

[46] See page 11, lines 24-26; and FIG. 2, element SM4

[47] See page 11, lines 26-27.

[48] See page 11, lines 24-26; and FIG. 2, element SM4

[49] See page 8, lines 7-11; and FIG. 2, element MAE.

[50] See page 12, line 10; and FIG. 2, element SM5.

[51] See FIG. 2, element SM1.

alarm means[52], of a network observation means[53] and of the service level agreement management means[54], in accordance with at least some of said chosen assurance rules[55].

Claim 16 is directed to a device according to claim 15, wherein said monitoring means[56] are supplied with information data by said analysis means[57] and/or said network observation means[58] and/or the service level agreement management means (SM4), and are arranged so as to order said alarm means[59] to generate alarms and/or reports in the event of detecting non-compliance with an assurance rule by received the information data.

Claim 17 is directed to a device according to claim 15, wherein said monitoring means[60] are arranged in the form of a rule engine storing said chosen assurance rules[61].

Claim 18 is directed to a device according to claim 15, wherein said monitoring means[62] are configurable[63].

[52] See FIG. 2, element SM2.

[53] See FIG. 2, element SM3.

[54] See FIG. 2, element SM4.

[55] See page 12, lines 11-16; and FIG. 2, elements SM1-SM4.

[56] See page 12, line 10; and FIG. 2, element SM5.

[57] See page 12, lines 10-16; and FIG. 2, element SM1.

[58] See page 12, lines 10-16; and FIG. 2, element SM3.

[59] See page 12, lines 10-16; and FIG. 2, element SM2.

[60] See page 12, line 10; and FIG. 2, element SM5.

[61] See page 12, lines 12-15.

[62] See page 12, line 10; and FIG. 2, element SM5.

Claim 19 is directed to a device according to claim 1, wherein said management means[64] are capable of being configured by said network management system[65] via an application programming interface[66] of said network element.

Claim 20 is directed to a device according to claim 1, wherein said management means[67] are capable of being configured by said network management system[68] via an application programming interface[69] of said network element[70] and via said management information base[71].

Claim 21 is directed to a device according to claim 19, wherein said analysis means[72] and/or said alarm means[73] and/or said network observation means[74] and/or said monitoring

[63] See page 13, lines 12-14.

[64] See page 8, lines 7-11; and FIG. 2, element MAE.

[65] See FIG. 2, element NMS.

[66] See page 15, lines 21-22; and FIG. 2, element API.

[67] See page 8, lines 7-11; and FIG. 2, element MAE.

[68] See FIG. 2, element NMS.

[69] See page 15, lines 21-22; and FIG. 2, element API.

[70] See FIG. 2, element NE.

[71] See page 15, lines 21-23; and FIG. 2, element MIB.

[72] See FIG. 2, element SM1.

[73] See FIG. 2, element SM2.

[74] See FIG. 2, element SM3.

means[75] and/or the service level agreement management means[76] are capable of being configured by said network management system[77], via said application programming interface[78].

Claim 22 is directed to a device according to claim 20, wherein said analysis means[79] and/or said alarm means[80] and/or said network observation means[81] and/or said monitoring means[82] and/or the service level agreement management means[83] are capable of being configured by said network management system[84], via said application programming interface and via said management information base[85].

Claim 23 is directed to a device according to claim 1, wherein said management means[86]are capable of being configured by said network management system[87] using dedicated commands[88].

[75] See FIG. 2, element SM5.

[76] See FIG. 2, element SM4.

[77] See page 15, line 25; and FIG. 2, element NMS.

[78] See page 15, lines 21-23; and FIG. 2, element API.

[79] See page 15, lines 21-23; and FIG. 2, element SM1.

[80] See page 15, lines 21-23; and FIG. 2, element SM2.

[81] See page 15, lines 21-23; and FIG. 2, element SM3.

[82] See page 15, lines 21-23; and FIG. 2, element SM5.

[83] See page 15, lines 21-23; and FIG. 2, element SM4.

[84] See page 15, line 25; and FIG. 2, element NMS.

[85] See page 15, lines 21-23.

[86] See page 8, lines 7-11; and FIG. 2, element MAE.

Claim 24 is directed to a device according to claim 23, wherein said analysis means[89] and/or said alarm means[90] and/or said network observation means[91] and/or said service level agreement management means[92] and/or said monitoring means[93] are arranged so as to be capable of being configured by said network management system[94] using dedicated commands[95].

Claim 26 is directed to a network element[96] for a communication network[97] equipped with a network management system[98], where said network element[99] presents a chosen configuration and including means for the measurement of parameter values[100] in the network[101] and a

[87] See FIG. 2, element NMS.

[88] See page 16, lines 5-8.

[89] See FIG. 2, element SM1.

[90] See FIG. 2, element SM2.

[91] See FIG. 2, element SM3.

[92] See FIG. 2, element SM4.

[93] See FIG. 2, element SM5.

[94] See FIG. 2, element NMS.

[95] See page 16, lines 5-8.

[96] See FIG. 2, element NE; and page 8, lines 3-7.

[97] See FIG. 1, element N; and page 6, lines 4-10.

[98] See FIG. 1, element NMS; and page 6, lines 10-11.

[99] See FIG. 2, element NE.

[100] See FIG. 2, element MM.

[101] See page 7, lines 20-23.

management information base[102] capable of storing management data representing said parameter values, wherein the network element comprises a device or arrangement (D)[103] in accordance with claim 1.

Claim 27 is directed to a network element in accordance with claim 26, further comprising an application programming interface[104], and wherein said management information base[105] is capable of being configured by said network management system[106] via said application programming interface[107].

Claim 28 is directed to a network element in accordance with claim 26, further comprising an application programming interface[108], and wherein said management information base is capable of being programmed by said network management system via said application programming interface[109].

Independent claim 32 is directed to a method of managing network technologies comprising:

[102] See FIG. 2, element MIB.

[103] See FIG. 2, element D; and page 8, line 2.

[104] See page 15, lines 21-22; and FIG. 2, element API.

[105] See page 15, lines 21-23; and FIG. 2, element MIB.

[106] See page 15, line 25; and FIG. 2, element NMS.

[107] See page 15, lines 21-23; and FIG. 2, element API.

[108] See page 15, lines 21-22; and FIG. 2, element API.

[109] See page 15, lines 23-25; and FIG. 2, element API.

applying a local assurance management device[110] for a network element[111] in a communication network[112] equipped with a network management system[113],

wherein said network element presents a chosen configuration[114] and comprises means for measuring parameter values[115] in the network[116], and a built-in management information base[117] used to store management data which are representative of said measured parameter values[118], and

wherein the device comprises management means[119] which are arranged to adapt the configuration of said network element[120] according to at least said management data stored in said management information base[121], and chosen rules, known as assurance rules, defining a

[110] See FIG. 2, element D; and page 8, line 2.

[111] See FIG. 2, element NE; and page 8, lines 3-7.

[112] See FIG. 1, element N; and page 6, lines 4-10.

[113] See page 8, line 34 - page 9, line 3.

[114] See page 10, lines 33-34.

[115] See page 7, lines 11-30; and FIG. 2, element MM.

[116] See page 11, lines 12-13.

[117] See FIG. 2, element MIB.

[118] See page 6, lines 14-16.

[119] See page 8, lines 7-11; and FIG. 2, element MAE.

[120] See page 8, lines 7-11; and FIG. 2, element MAE.

[121] See page 8, lines 15-21; and FIG. 2, element MIB.

local assurance policy[122], where said adaptation comprises a change to a measurement policy parameter and/or a change to a report transmission policy to said network management system[123].

[122] See page 8, lines 11-12.

[123] See page 8, lines 15-21; and FIG. 2, element NMS.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-33 stand rejected under 35 U.S.C. 102(e) as being allegedly anticipated by Sistanizadeh et al. (U.S. 6,681,232; hereinafter "Sistanizadeh").

VII. ARGUMENT

For each ground of rejection, the claims do not stand or fall together but are patentable on separate grounds as forth below.

1. Rejection of Claims 1-33 based on Sistanizadeh

Claim 1

Appellants respectfully submit that claim 1 is not anticipated by Sistanizadeh.

Claim 1 recites, in part:

> a built-in management information base used to ***store management data which are representative of said measured parameter values***, wherein the device comprises management means which are arranged to adapt the configuration of said network element according to at least said management data stored in said management information base.

The Examiner in the Advisory Action asserts:

> an SNMP agent stores and retrieves management data as defined by the MIB (column 16, lines 25-25), furthermore, the managed data of Sistanizadeh includes data from, "The measurement service module 161 [which] looks at the raw data from the various monitoring devices, as accumulated by the monitoring service 157" (column 19, lines 5-7), whereby the modules are a part of "the SLM application server 107 relies on a Relational Database 109, which contains information on the Network and Service Topologies, network and service metrics, SLA parameters, customer demarcation points, service scope and boundaries, etc" (column 7, lines 41-44),

as disclosing "management data which are representative of said measured parameter values." (See Advisory Action mailed September 10, 2008, page 2). Based on the above comments, the Examiner has failed to respond to the crux of the argument presented in the Amendment filed August 22, 2008. In Sistanizadeh, the modules 161 are part of the SLM application plane (see col. 19, line 60, and FIG. 7). Contrary to the Examiner's assertion, FIG. 7 of Sistanizadeh does not teach or suggest that the measurement service module 161 is a part of the SLM application server 107. Furthermore, the subscriber chooses how much bandwidth to purchase. (See col. 21, lines 36-37). In response to the choice by the subscriber, the provisioning service module 151 instructs ***the management module 165 to allocate reserved resources*** to the particular customer's service. In response, the management module 165 instructs the agent(s) in the affected switch(es) to make the necessary configuration changes to provide the increased bandwidth service for the port(s) of the particular customer. (See col. 21, lines 45-51). Accordingly, the management module of Sistanizadeh is unrelated to the "management data" as recited in the claimed invention, as the management module of Sistanizadeh allocates bandwidth in response to a subscriber's demand. In the present invention, however, the management data are representative of said measured parameter values. Thus, the management module of Sistanizadeh does not disclose or suggest, "management data", as claimed.

Claim 1 also recites, in part:

> the device comprises management means which are arranged to adapt the configuration of said network element according to…chosen rules, known as assurance rules, defining a local assurance policy, where said adaptation comprises a change to ***a measurement policy parameter*** and/or a change to a report transmission policy to said network management system.

In the Advisory Action, the Examiner asserts that Sistanizadeh discloses a change to the measurement policy as "QoS monitoring/reporting and automatic bandwidth increases/decreases" (see col. 17, lines 50-53). In Sistanizadeh, however, "QoS monitoring/reporting and automatic bandwidth increases/decreases" relates to service layer and network management layer services. (See col. 17, lines 50-53). Sistanizadeh, however, does not teach or suggest that "the QoS monitoring/reporting and automatic bandwidth increases/decreases" corresponds to "where said adaptation comprises a change to a ***measurement policy parameter***" as recited in claim 1.

Claim 1 also recites, in part:

> the device comprises management means which are arranged to adapt the configuration of said network element according to...chosen rules, known as assurance rules, defining a local assurance policy, where said adaptation comprises a change to a measurement policy parameter and/or a change to a report transmission policy to said network management system.

The Examiner asserts that the "local assurance policy" as recited in claim 1, is disclosed at col. 17, lines 56-61 of Sistanizadeh where the *SLM* anticipates a local assurance policy by the SLM. Appellants respectfully disagree with the Examiner's position.

In Sistanizadeh, the SLM application monitors the health of the network by analyzing semantic transparency and time transparency of data and control traffic through the network and provides the results of this analysis to various users, such as network service customers and network operations personnel. Furthermore, the SLM application offers a provisioning service which increases or decreases bandwidth. (See col. 18, lines 49-53). Nowhere in Sistanizadeh, however, does the "SLM" in Sistanizadeh disclose "adapt[ing] the configuration of said network element according to...chosen rules, known as assurance rules, defining a local assurance policy" as recited in claim 1. Specifically, Sistanizadeh is not at all concerned with a local assurance policy.

Appellants refer the Examiner to, for example, page 8, lines 21-27 and page 14, lines 6-30, of the Appellants' specification which discusses a local assurance policy. Therefore, in light of the Appellants' specification, it would be clear to one of ordinary skill in the art that Sistanizadeh does not disclose a local assurance policy.

In view of the above deficiencies, Appellants submit that independent claim 1 is patentable over Sistanizadeh.

Claim 2

Appellants submit that dependent claim 2 is patentable at least by virtue of its dependency on claim 1.

Claim 2 recites, in part, "management means are arranged so as to adapt said configuration according to information data coming from at least one other network element". The Examiner asserts, "Sistanizadeh discloses the adaptation of the configuration data coming from at least one other network element (column 18, lines 56-59, where the *provisioning service* anticipates the information data coming from another network element as a result of submitting *the information to the relevant devices in the network)*". The "provisioning service" of Sistanizadeh, however, "***submits*** the information to the relevant device in the network plane equipment" but does not disclose or suggest, "adapt said configuration according to information data ***coming from*** at least one other network element" as recited in claim 2. Thus, claim 2 should be deemed allowable.

Claim 3

Appellants submit that dependent claim 3 is patentable at least by virtue of its dependency on claim 1.

Claim 3 recites, in part, "wherein said adaptation comprises a change to a method of operation of said network element". In the Advisory Action, the Examiner argues:

> Sistanizadeh disclosure of changing the bandwidth per an operation of the customer (col. 29, lines 40-46, start of a File Transfer Protocol) anticipates a change in method of operation, not merely because the amount of bandwidth simply changed, but rather because the type and level of service changed to accommodate the operation (col. 28, lines 40-46, provide a guaranteed bandwidth with minimum jitter dynamically at the detected start of a voice over IP session).

Based on the Examiner's comments, the Examiner has maintained that changing the bandwidth per a customer demand corresponds to a change to a method of operation of said network element. Changing the bandwidth of the agent in Sistanizadeh, however, does not disclose "wherein said adaptation comprises a change to a method of operation of said network element" as claimed. In Sistanizadeh, the utility service performs graceful shutdown and restart. (See col. 19, line 39). Such an operation as disclosed in Sistanizadeh is a support function performed by the utility service 163. (See col. 19, line 36). Thus, performing the shutdown and restart in Sistanizadeh, would not constitute a "***change to a method of operation*** of said network element" as recited in claim 3.

Sistanizadeh, however, changes the bandwidth per a customer demand, but changing the bandwidth of the agent does not disclose "wherein said adaptation comprises a change to a method of operation of said network element" as claimed. Therefore, claim 3 should be deemed allowable.

Claim 4

Appellants submit that dependent claim 4 is patentable at least by virtue of its dependency on claim 1.

Claim 4 recites in part:

> analysis means arranged so as to determine, in accordance with certain of said chosen assurance rules, information data representing the changes in time, over a chosen interval, of parameter values in the network stored in said management information base.

The Examiner maintains that col. 21, lines 7-14, and col. 25, lines 20-25 of Sistanizadeh disclose the above recited features. Sistanizadeh, however, teaches that the measurement module 161 computes the report statistics for the particular customer from ***the raw data*** from latency agents, (see col. 21, lines 7-14), and the latency agents identify and report latency violations (see col. 25, lines 20-25). The Examiner argues in the Final Office Action dated May 22, 2008, that the "latency agent anticipates the chosen assurance rules as a result of an alarm triggered a respective threshold value is exceeded", however, an alarm being triggered does not teach or suggest that the "in accordance with certain of said chosen assurance rules, information data representing the changes in time". Therefore, claim 4 should be deemed allowable.

Claims 5-31

Appellants submit that dependent claims 5-31 are patentable at least by virtue of its dependency on claim 1.

Claim 32

Further, for the same reasons that claim 1 is patentable over the prior art, claim 32 is also patentable over the prior art as claim 32 recites similar claim features as claim 1, but in a method format.

Claim 33

Appellants submit that dependent claim 33 is patentable at least by virtue of its dependency on claim 32.

Conclusion

The USPTO is directed and authorized to charge the statutory fee (37 C.F.R. §41.37(a) and 1.17(c)) and all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

/Theodore C. Shih/

Theodore C. Shih
Registration No. 60,645

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: January 9, 2009

CLAIMS APPENDIX

CLAIMS 1-33 ON APPEAL:

1. A local assurance management device for a network element in a communication network equipped with a network management system, where said network element presents a chosen configuration and comprises means for measuring parameter values in the network, and a built-in management information base used to store management data which are representative of said measured parameter values, wherein the device comprises
management means which are arranged to adapt the configuration of said network element according to at least said management data stored in said management information base, and chosen rules, known as assurance rules, defining a local assurance policy, where said adaptation comprises a change to a measurement policy parameter and/or a change to a report transmission policy to said network management system.

2. A device according to claim 1, wherein said management means are arranged so as to adapt said configuration according to information data coming from at least one other network element.

3. A device according to claim 1, wherein said adaptation comprises a change to a method of operation of said network element.

4. A device according to claim 1, wherein said management means include analysis means arranged so as to determine, in accordance with certain of said chosen assurance rules, information data representing the changes in time, over a chosen interval, of parameter values in the network stored in said management information base.

5. A device according to claim 4, wherein said analysis means are arranged so as to deliver information data representing a trend analysis and/or an analysis of profiles or signatures and/or an analysis of discontinuity and/or an aggregation of network parameter values.

6. A device according to claim 4, wherein said analysis means are configurable.

7. A device according to claim 6, wherein said analysis means are arranged so as perform fresh calculations relating to the network parameters received from said network management system.

8. A device according to claim 1, wherein said management means include alarm means able to trigger the sending of an alarm and/or of information data to said network management system

and/or to at least one other network element, in accordance with certain of said chosen assurance rules.

9. A device according to claim 8, wherein said alarm means are configurable.

10. A device according to claim 8, wherein said information data and said alarms are representative of the results of analyses performed by an analysis means, and/or of data aggregation, effected by said analysis means, and/or of a network parameter value stored in said management information base.

11. A device according to claim 1, wherein said management means include network observation means defining a flow measurement agent of the end-to-end type, arranged so as to determine information data which are representative of said flow of the end-to-end type in accordance with certain of said chosen assurance rules.

12. A device according to claim 11, wherein said network observation means are configurable.

13. A device according to claim 1, wherein said management means include means for the management of service level agreements or SLAs, arranged so as to determine information data representing said agreement management in accordance with certain of said chosen assurance rules.

14. A device according to claim 13, wherein said service level agreement management means are configurable.

15. A device according to claim 2, wherein said management means include monitoring means which are able to manage the operation of an analysis means, of an alarm means, of a network observation means and of the service level agreement management means, in accordance with at least some of said chosen assurance rules.

16. A device according to claim 15, wherein said monitoring means are supplied with information data by said analysis means and/or said network observation means and/or the service level agreement management means (SM4), and are arranged so as to order said alarm means to generate alarms and/or reports in the event of detecting non-compliance with an assurance rule by received the information data.

17. A device according to claim 15, wherein said monitoring means are arranged in the form of a rule engine storing said chosen assurance rules.

18. A device according to claim 15, wherein said monitoring means are configurable.

19. A device according to claim 1, wherein said management means are capable of being configured by said network management system via an application programming interface of said network element.

20. A device according to claim 1, wherein said management means are capable of being configured by said network management system via an application programming interface of said network element and via said management information base.

21. A device according to claim 19, wherein said analysis means and/or said alarm means and/or said network observation means and/or said monitoring means and/or the service level agreement management means are capable of being configured by said network management system, via said application programming interface.

22. A device according to claim 20, wherein said analysis means and/or said alarm means and/or said network observation means and/or said monitoring means and/or the service level agreement management means are capable of being configured by said network management system, via said application programming interface and via said management information base.

23. A device according to claim 1, wherein said management means are capable of being configured by said network management system using dedicated commands.

24. A device according to claim 23, wherein said analysis means and/or said alarm means and/or said network observation means and/or said service level agreement management means and/or said monitoring means are arranged so as to be capable of being configured by said network management system using dedicated commands.

25. A device according to claim 23, wherein said commands are of the "Command Line Interface" type.

26. A network element for a communication network equipped with a network management system, where said network element presents a chosen configuration and including means for the measurement of parameter values in the network and a management information base capable of storing management data representing said parameter values, wherein the network element comprises a device or arrangement (D) in accordance with claim 1.

27. A network element in accordance with claim 26, further comprising an application programming interface, and wherein said management information base is capable of being configured by said network management system via said application programming interface.

28. A network element in accordance with claim 26, further comprising an application programming interface, and wherein said management information base is capable of being programmed by said network management system via said application programming interface.

29. A network element in accordance with claim 26, wherein the network element is chosen from a group which includes at least one of routers, switches and firewalls.

30. A communication network according to claim 26, comprising a network management system, wherein the communication network comprises a plurality of different network elements comprising at least one of a server equipped with a firewall, a switch, an edge router or a core router.

31. A network in accordance with claim 30, wherein each network element is arranged to deliver alarms and/or information data of various types to said network management system.

32. A method of managing network technologies comprising:
applying a local assurance management device for a network element in a communication network equipped with a network management system,

wherein said network element presents a chosen configuration and comprises means for measuring parameter values in the network, and a built-in management information base used to store management data which are representative of said measured parameter values, and
wherein the device comprises management means which are arranged to adapt the configuration of said network element according to at least said management data stored in said management information base, and chosen rules, known as assurance rules, defining a local assurance policy, where said adaptation comprises a change to a measurement policy parameter and/or a change to a report transmission policy to said network management system.

33. A method according to claim 32, wherein said network technologies are chosen from a group which includes transmission networks, comprising at least one of a Wavelength-Division Multiplexing, a Synchronous Optical NETwork and a Synchronous Digital Hierarchy type, management networks, of the Internet-IP and Asynchronous Transfer Mode type, and speech networks, of the conventional, mobile and Next Generation Network type.

EVIDENCE APPENDIX:

Appellants are not submitting any evidence pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or any other evidence entered by the Examiner and relied upon by Appellants in the appeal.

RELATED PROCEEDINGS APPENDIX

Submitted herewith are copies of decisions rendered by a court or the Board in any proceeding identified about in Section II pursuant to 37 C.F.R. § 41.37(c)(1)(ii).

Copy of Notice of Panel Decision from Pre-Appeal Brief Review dated December 9, 2008.

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of	Docket No: Q80686
Emmanuel MARILLY, et al.	
Appln. No.: 10/809,521	Group Art Unit: 2157
Confirmation No.: 7535	Examiner: Blake J. RUBIN
Filed: March 26, 2004	

For: A LOCAL ASSURANCE MANAGEMENT DEVICE FOR AN EQUIPMENT ELEMENT IN A COMMUNICATION NETWORK

SUBMISSION OF APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith please find an Appeal Brief. The USPTO is directed and authorized to charge the statutory fee of $540.00 and all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

/Theodore C. Shih/

Theodore C. Shih
Registration No. 60,645

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: January 9, 2009